

CLAIMS

1 1. A method for satisfiability (SAT) testing, given a
2 set of formulas describing a target system, the formulas
3 including clauses that include variables and express
4 constraints on states of the system, the set of the
5 formulas including at least a first and a second formula,
6 the method comprising:

7 analyzing the first formula so as to deduce one or
8 more conflict clauses, each such conflict clause
9 expressing assignments of the variables that prevent a
10 respective conflict, subject to which the first formula
11 cannot be satisfied, while determining, for each of the
12 conflict clauses, the clauses in the first formula that
13 lead to the respective conflict;

14 identifying the conflict clauses for which the
15 clauses that lead to the respective conflict in the first
16 formula are a subset of the clauses in the second
17 formula; and

18 analyzing the second formula subject to the
19 identified conflict clauses, in order to determine
20 whether the second formula can be satisfied.

1 2. A method according to claim 1, wherein the clauses
2 are formulated in a conjunctive normal form (CNF), and
3 wherein analyzing the second formula comprises forming a
4 conjunction of the CNF of the second formula with the
5 identified conflict clauses, and solving the conjunction.

1 3. A method according to claim 1, wherein analyzing the
2 first formula comprises determining while analyzing the
3 first formula whether, for each of the conflict clauses,
4 the clauses that lead to the respective conflict are in
5 the subset of the clauses in the second formula.

1 4. A method according to claim 1, wherein the set of
2 formulas comprises a sequence of bounded model checking
3 (BMC) instances, and wherein analyzing the first and
4 second formulas comprises solving the BMC instances.

1 5. A method for bounded model checking (BMC) of a
2 target system, comprising:

3 generating a succession of BMC instances describing
4 the target system in the form of propositional
5 satisfiability (SAT) formulas, the formulas comprising
6 clauses that comprise variables and express constraints
7 on states of the system;

8 analyzing a first instance in the succession of the
9 BMC instances while deriving one or more conflict clauses
10 that forbid certain assignments of the variables that
11 give rise to conflicts, subject to which the first
12 instance cannot be satisfied;

13 for each of the instances in the succession
14 subsequent to the first instance, identifying the
15 conflict clauses derived in a preceding one of the
16 instances that are also pertinent to the subsequent
17 instance; and

18 solving the subsequent instance subject to the
19 identified conflict clauses, so as to seek a satisfying
20 assignment of the variables, such that when a satisfying
21 assignment is not found at the subsequent instance, one
22 or more further conflict clauses are derived for use in
23 solving a further one of the instances in the sequence.

1 6. A method according to claim 5, wherein identifying
2 the conflict clauses comprises finding the conflict
3 clauses that are induced by the clauses in the preceding

4 one of the instances that are also comprised in the
5 subsequent instance.

1 7. A method according to claim 5, wherein solving the
2 subsequent instance comprises solving the subsequent
3 instance subject to substantially all of the conflict
4 clauses identified as pertinent to the subsequent
5 instance in a plurality of the instances in the sequence
6 prior to the subsequent instance.

1 8. A method according to claim 5, wherein generating
2 the succession of BMC instances comprises defining a
3 model and a safety property of the target system, and
4 wherein solving each of the instances comprises finding a
5 violation of the safety property corresponding to the
6 satisfying assignment.

1 9. A method according to claim 5, wherein generating
2 the succession of BMC instances comprises formulating the
3 logical clauses in a conjunctive normal form (CNF), and
4 wherein solving the subsequent instance comprises forming
5 a conjunction of the CNF of the subsequent instance with
6 the identified conflict clauses, and solving the
7 conjunction.

1 10. Apparatus for satisfiability (SAT) testing,
2 comprising a satisfiability processor, which is arranged
3 to receive a set of formulas describing a target system,
4 the formulas comprising clauses that comprise variables
5 and express constraints on states of the system, the set
6 of the formulas comprising at least a first and a second
7 formula, the processor being further arranged to analyze
8 the first formula while deducing one or more conflict
9 clauses, each such conflict clause prevent assignments

10 of the variables that give rise to a respective conflict,
11 subject to which the first formula cannot be satisfied,
12 while determining, for each of the conflict clauses, the
13 clauses in the first formula that lead to the respective
14 conflict, and to identify the conflict clauses for which
15 the clauses that lead to the respective conflict in the
16 first formula are a subset of the clauses in the second
17 formula, the processor being still further arranged to
18 analyze the second formula subject to the identified
19 conflict clauses, in order to determine whether the
20 second formula can be satisfied.

1 11. Apparatus according to claim 10, wherein the set of
2 formulas are provided in a conjunctive normal form (CNF),
3 and wherein the processor is arranged to analyze the
4 second formula by forming a conjunction of the CNF of the
5 second formula with the identified conflict clauses, and
6 solving the conjunction.

1 12. Apparatus according to claim 10, wherein the
2 processor is arranged to determine while analyzing the
3 first formula whether, for each of the conflict clauses,
4 the clauses that lead to the respective conflict are in
5 the subset of the clauses in the second formula.

1 13. Apparatus according to claim 10, wherein the set of
2 formulas comprises a sequence of bounded model checking
3 (BMC) instances.

1 14. Apparatus for bounded model checking (BMC) of a
2 target system, comprising a verification processor, which
3 is arranged to receive a succession of BMC instances
4 describing the target system in the form of propositional
5 satisfiability (SAT) formulas, the formulas comprising

6 clauses that comprise variables and express constraints
7 on states of the system, the processor being further
8 arranged to analyze a first instance in the succession of
9 the BMC instances while deriving one or more conflict
10 clauses that forbid certain assignments of the variables
11 that give rise to conflicts, subject to which the first
12 instance cannot be satisfied, and to identify, for each
13 of the instances in the succession subsequent to the
14 first instance, the conflict clauses derived in a
15 preceding one of the instances that are also pertinent to
16 the subsequent instance, the processor being still
17 further arranged to solve the subsequent instance subject
18 to the identified conflict clauses, so as to seek a
19 satisfying assignment of the variables, such that when a
20 satisfying assignment is not found at the subsequent
21 instance, the processor derives one or more further
22 conflict clauses for use in solving a further one of the
23 instances in the sequence.

1 15. Apparatus according to claim 14, wherein the
2 processor is arranged to identify the conflict clauses
3 that are also pertinent to the subsequent instance by
4 finding the conflict clauses that are induced by the
5 clauses in the preceding one of the instances that are
6 also comprised in the subsequent instance.

1 16. Apparatus according to claim 14, wherein the
2 processor is arranged to solve the subsequent instance
3 subject to substantially all of the conflict clauses
4 identified as pertinent to the subsequent instance in a
5 plurality of the instances in the sequence prior to the
6 subsequent instance.

1 17. Apparatus according to claim 14, wherein the
2 succession of BMC instances are defined by a model and a
3 safety property of the target system, and wherein the
4 processor is arranged, by solving each of the instances,
5 to find a violation of the safety property corresponding
6 to the satisfying assignment.

1 18. Apparatus according to claim 14, wherein the
2 succession of BMC instances are formulated in a
3 conjunctive normal form (CNF), and wherein the processor
4 is arranged to solve the subsequent instance by forming a
5 conjunction of the CNF of the subsequent instance with
6 the identified conflict clauses, and solving the
7 conjunction.

1 19. A computer software product for satisfiability (SAT)
2 testing, comprising a computer-readable medium in which
3 program instructions are stored, which instructions, when
4 read by a computer, cause the computer to receive a set
5 of formulas describing a target system, the formulas
6 comprising clauses that comprise variables and express
7 constraints on states of the system, the set of the
8 formulas comprising at least a first and a second
9 formula, and which instructions further cause the
10 computer to analyze the first formula while deducing one
11 or more conflict clauses, each such conflict clause
12 expressing assignments of the variables that prevent a
13 respective conflict, subject to which the first formula
14 cannot be satisfied, while determining, for each of the
15 conflict clauses, the clauses in the first formula that
16 lead to the respective conflict, and to identify the
17 conflict clauses for which the clauses that lead to the
18 respective conflict in the first formula are a subset of

19 the clauses in the second formula, and to analyze the
20 second formula subject to the identified conflict
21 clauses, in order to determine whether the second formula
22 can be satisfied.

1 20. A product according to claim 19, wherein the set of
2 formulas are provided in a conjunctive normal form (CNF),
3 and wherein the instructions cause the computer to
4 analyze the second formula by forming a conjunction of
5 the CNF of the second formula with the identified
6 conflict clauses, and solving the conjunction.

1 21. A product according to claim 19, wherein the
2 instructions cause the computer to determine while
3 analyzing the first formula whether, for each of the
4 conflict clauses, the clauses that lead to the respective
5 conflict are in the subset of the clauses in the second
6 formula.

1 22. A product according to claim 19, wherein the set of
2 formulas comprises a sequence of bounded model checking
3 (BMC) instances.

1 23. A computer software product for bounded model
2 checking (BMC) of a target system, comprising a
3 computer-readable medium in which program instructions
4 are stored, which instructions, when read by a computer,
5 cause the computer to receive a succession of BMC
6 instances describing the target system in the form of
7 propositional satisfiability (SAT) formulas, the formulas
8 comprising clauses that comprise variables and express
9 constraints on states of the system, and further cause
10 the computer to analyze a first instance in the
11 succession of the BMC instances while deriving one or

12 more conflict clauses that forbid certain assignments of
13 the variables that give rise to conflicts, subject to
14 which the first instance cannot be satisfied, and to
15 identify, for each of the instances in the succession
16 subsequent to the first instance, the conflict clauses
17 derived in a preceding one of the instances that are also
18 pertinent to the subsequent instance, and which still
19 further cause the computer to solve the subsequent
20 instance subject to the identified conflict clauses, so
21 as to seek a satisfying assignment of the variables, such
22 that when a satisfying assignment is not found at the
23 subsequent instance, the computer derives one or more
24 further conflict clauses for use in solving a further one
25 of the instances in the sequence.

1 24. A product according to claim 23, wherein the
2 instructions cause the computer to identify the conflict
3 clauses that are also pertinent to the subsequent
4 instance by finding the conflict clauses that are induced
5 by the clauses in the preceding one of the instances that
6 are also comprised in the subsequent instance.

1 25. A product according to claim 23, wherein the
2 instructions cause the computer to solve the subsequent
3 instance subject to substantially all of the conflict
4 clauses identified as pertinent to the subsequent
5 instance in a plurality of the instances in the sequence
6 prior to the subsequent instance.

1 26. A product according to claim 23, wherein the
2 succession of BMC instances are defined by a model and a
3 safety property of the target system, and wherein the
4 instructions cause the computer, by solving each of the

40967S3

5 instances, to find a violation of the safety property
6 corresponding to the satisfying assignment.

1 27. A product according to claim 23, wherein the
2 succession of BMC instances are formulated in a
3 conjunctive normal form (CNF), and wherein the
4 instructions cause the computer to solve the subsequent
5 instance by forming a conjunction of the CNF of the
6 subsequent instance with the identified conflict clauses,
7 and solving the conjunction.

TOGETHER